



UNITED STATES MARINE CORPS
MARINE CORPS SYSTEMS COMMAND
2200 LESTER STREET
QUANTICO, VIRGINIA 22134-5010

IN REPLY REFER TO:

5720
DON-USMC-20-007255
20 May 20

EMAILED TO: *foia@foia.com*

Ms. Rose Santos
FOIA GROUP
PO Box 368
Depew NY 14043

SUBJECT: DON-USMC-2020-007255

Dear Ms. Santos:

This letter responds to your Freedom of Information Act request dated April 28, 2020, requesting a copy of Task/Delivery Order M67854-20-F-4003, including the Statement of Work as well as all modifications.

In light of the *MCI Worldcom, Inc, v. GSA* decision, the Department of Justice Office of Information and Privacy has advised the Navy Office of the General Counsel that submitter notification in accordance with Executive Order 12,600 should be made whenever an agency receives a FOIA request for documents that contain potentially confidential information in order to obtain and consider any objections to disclosure. Therefore, in accordance with Presidential Executive Order 12,600, we allowed the submitter to review the requested documents and provide comment.

Pursuant to the aforementioned Executive Order 12,600 request, the submitter has no objection to the full release of the requested documents.

Fees associated with processing your request are minimal and waived.

If at any time you are not satisfied that a diligent effort was made to process your request, you may file an administrative appeal with the Assistant to the General Counsel (FOIA) at:

Department of the Navy
Office of the General Counsel
ATTN: FOIA Appeals Office
1000 Navy Pentagon Room 4E635
Washington DC 20350-1000


DON-USMC-2020-007255


Page 2 of 2

20 May 20

Any questions concerning this matter should be directed to Mrs. Bobbie Cave at (703) 432-3934 or bobbie.cave@usmc.mil.

Sincerely,


for Lisa L. Baker
Counsel

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS <i>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30</i>				1. REQUISITION NUMBER M0008920SUPKILB		PAGE 1 OF 45	
2. CONTRACT NO. 47QTC18D0007		3. AWARD/EFFECTIVE DATE 31-Oct-2019		4. ORDER NUMBER M6785420F4003		5. SOLICITATION NUMBER	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME				b. TELEPHONE NUMBER (No Collect Calls)	
8. OFFER DUE DATE/LOCAL TIME							
9. ISSUED BY COMMANDER, MARINE CORPS SYSTEMS COMMAND ATTN: MS. NATASHA JONES 2200 LESTER STREET QUANTICO VA 22134-6050 TEL: (703) 432-2823 FAX:		CODE M67854		10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: _____ % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> EDWOSB NAICS: 541519 SIZE STANDARD: \$30,000,000			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS Net 30 Days		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING	
15. DELIVER TO MARINE CORPS CYBERSPACE OPERATIONS GROUP DAWN CAPERS BLDG 27410 HOT PATCH ROAD QUANTICO VA 22134-5046		CODE M00089		16. ADMINISTERED BY SEE ITEM 9			
17a. CONTRACTOR/OFFEROR SMARTRONIX, INC. 44150 SMARTRONIX WAY HOLLYWOOD MD 20636-3172 TELEPHONE NO. (301) 373-6000 X328		CODE 03MT8 FACILITY CODE		18a. PAYMENT WILL BE MADE BY DFAS COLUMBUS DEFENSE FINANCE & ACCOUNTING SERVICE COLUMBUS DFAS-JDCBB/CO PO BOX 182317 COLUMBUS OH 43218-2317			
17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER <input type="checkbox"/>		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED <input checked="" type="checkbox"/> SEE ADDENDUM					
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES			21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
SEE SCHEDULE							
25. ACCOUNTING AND APPROPRIATION DATA See Schedule						26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$2,474,651.75	
27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED							
27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED							
28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED. <input checked="" type="checkbox"/>				29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: <input type="checkbox"/>			
30a. SIGNATURE OF OFFEROR/CONTRACTOR				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) 			
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)		30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) ALEXANDER E. LYON / CONTRACTING OFFICER TEL: 703-432-4369 EMAIL: alexander.lyon@usmc.mil		31c. DATE SIGNED 31-Oct-2019	

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS (CONTINUED)				PAGE 2 OF 45	
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				
32a. QUANTITY IN COLUMN 21 HAS BEEN <input type="checkbox"/> RECEIVED <input type="checkbox"/> INSPECTED <input type="checkbox"/> ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____					
32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE			32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
			32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
33. SHIP NUMBER <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL		34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	
37. CHECK NUMBER					
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY			
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT 41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER		41c. DATE	42a. RECEIVED BY <i>(Print)</i>		
			42b. RECEIVED AT <i>(Location)</i>		
			42c. DATE REC'D <i>(YY/MM/DD)</i>	42d. TOTAL CONTAINERS	

Section SF 1449 - CONTINUATION SHEET

BOX 27B

The contract writing system does not allow Box 27b of the SF1449 to be checked. Box 27b is applicable, and FAR 52.212-4 and 52.212.5 are incorporated by reference.

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Public Key Infrastructure FFP Public Key Infrastructure support in accordance with the Performance Work Statement FOB: Destination MILSTRIP: M0008920SUPKILB PURCHASE REQUEST NUMBER: M0008920SUPKILB PSC CD: D301	6	Months	\$409,371.67	\$2,456,230.02
NET AMT					\$2,456,230.02
ACRN AA CIN: M0008920SUPKILB0001					\$2,456,230.02
0002	Public Key Infrastructure - Option FFP Public Key Infrastructure support in accordance with the Performance Work Statement FOB: Destination PSC CD: D301	6	Months	\$409,371.67	\$2,456,230.02
OPTION					
NET AMT					\$2,456,230.02

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003		1	Each	\$18,421.73	\$18,421.73
	Contractor Access Fee (CAF)				
	FFP				
	CAF for CLIN 0001 as required by GSA Alliant 2.				
	FOB: Destination				
	MILSTRIP: M0008920SUPKILB				
	PURCHASE REQUEST NUMBER: M0008920SUPKILB				
	PSC CD: D301				

NET AMT	\$18,421.73
---------	-------------

ACRN AA	\$18,421.73
CIN: M0008920SUPKILB0003	

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004		1	Each	\$18,421.73	\$18,421.73
OPTION	Contractor Access Fee (CAF)				
	FFP				
	CAF for CLIN 0002 as required by GSA Alliant 2.				
	FOB: Destination				
	PSC CD: D301				

NET AMT	\$18,421.73
---------	-------------

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	Destination	Government	Destination	Government
0002	Destination	Government	Destination	Government
0003	Destination	Government	Destination	Government
0004	Destination	Government	Destination	Government

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS	DODAAC / CAGE
0001	POP 01-NOV-2019 TO 30-APR-2020	N/A	MARINE CORPS CYBERSPACE OPERATIONS GROUP DAWN CAPERS BLDG 27410 HOT PATCH ROAD QUANTICO VA 22134-5046 (703) 784-2622 FOB: Destination	M00089
0002	POP 01-MAY-2020 TO 31-OCT-2020	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	M00089
0003	POP 01-NOV-2019 TO 30-APR-2020	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	M00089
0004	POP 01-MAY-2020 TO 31-OCT-2020	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	M00089

ACCOUNTING AND APPROPRIATION DATA

AA: 17011061CCY 254 67925 067443 2D 1CCY
COST CODE: 0SUPKILBCTDP
AMOUNT: \$2,474,651.75

ACRN	CLIN/SLIN	CIN	AMOUNT
AA	0001	M0008920SUPKILB0001	\$2,456,230.02
	0003	M0008920SUPKILB0003	\$18,421.73

CLAUSES INCORPORATED BY FULL TEXT

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days before Contract expiration.

(End of clause)

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (DEC 2018)

(a) Definitions. As used in this clause—

“Department of Defense Activity Address Code (DoDAAC)” is a six position code that uniquely identifies a unit, activity, or organization.

“Document type” means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

“Local processing office (LPO)” is the office responsible for payment certification when payment certification is done external to the entitlement system.

“Payment request” and “receiving report” are defined in the clause at 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(b) Electronic invoicing. The WAWF system provides the method to electronically process vendor payment requests and receiving reports, as authorized by Defense Federal Acquisition Regulation Supplement (DFARS) 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall—

(1) Have a designated electronic business point of contact in the System for Award Management at <https://www.sam.gov>; and

(2) Be registered to use WAWF at <https://wawf.eb.mil/> following the step-by-step procedures for self-registration available at this web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the “Web Based Training” link on the WAWF home page at <https://wawf.eb.mil/>.

(e) WAWF methods of document submission. Document submissions may be via web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF payment instructions. The Contractor shall use the following information when submitting payment requests and receiving reports in WAWF for this contract or task or delivery order:

(1) Document type. The Contractor shall submit payment requests using the following document type(s):

(i) For cost-type line items, including labor-hour or time-and-materials, submit a cost voucher.

(ii) For fixed price line items—

(A) That require shipment of a deliverable, submit the invoice and receiving report specified by the Contracting Officer.

(Contracting Officer: Insert applicable invoice and receiving report document type(s) for fixed price line items that require shipment of a deliverable.)

(B) For services that do not require shipment of a deliverable, submit either the Invoice 2in1, which meets the requirements for the invoice and receiving report, or the applicable invoice and receiving report, as specified by the Contracting Officer.

2in1

(iii) For customary progress payments based on costs incurred, submit a progress payment request.

(iv) For performance based payments, submit a performance based payment request.

(v) For commercial item financing, submit a commercial item financing request.

(2) Fast Pay requests are only permitted when Federal Acquisition Regulation (FAR) 52.213-1 is included in the contract.

[Note: The Contractor may use a WAWF “combo” document type to create some combinations of invoice and receiving report in one step.]

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table*

<i>Field Name in WAWF</i>	<i>Data to be entered in WAWF</i>
Pay Official DoDAAC	M00089
Issue By DoDAAC	M67854
Admin DoDAAC**	M67854
Inspect By DoDAAC	M00089
Ship To Code	_____
Ship From Code	_____
Mark For Code	M00089
Service Approver (DoDAAC)	M00089
Service Acceptor (DoDAAC)	M00089
Accept at Other DoDAAC	_____
LPO DoDAAC	_____
DCAA Auditor DoDAAC	_____
Other DoDAAC(s)	_____

(4) Payment request. The Contractor shall ensure a payment request includes documentation appropriate to the type of payment request in accordance with the payment clause, contract financing clause, or Federal Acquisition Regulation 52.216-7, Allowable Cost and Payment, as applicable.

(5) Receiving report. The Contractor shall ensure a receiving report meets the requirements of DFARS Appendix F.

(g) WAWF point of contact.

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

TBD

(Contracting Officer: Insert applicable information or "Not applicable.")

(2) Contact the WAWF helpdesk at 866-618-5988, if assistance is needed.

(End of clause)

SECTION C

Performance Work Statement (PWS) Marine Corps Cyberspace Operations Group (MCCOG) Public Key Infrastructure (PKI)

2.1 BACKGROUND

***Note – The PWS begins with paragraph 2.1.**

The United States Marine Corps is increasingly reliant on critical infrastructures and on computer and telecommunications systems to support essential information capabilities. The Marine Corps is committed to pursuing all necessary and prudent steps to ensure that Marine Corps communications and information technology are available to support Marines and civilian Marines, serving in both deployed and garrison environments, without compromising communications vulnerability.

Without exception, the goal of the Director of the Command, Control, Communications and Computers (C4) is to get the right information, to the right place, supported by highly skilled personnel delivering power to the edge for the warfighter. The Director of C4 is responsible for the development and oversight of policy, plans and guidance of information assurance. The Director C4 is the executive agent responsible for planning, directing, coordinating, and overseeing information assurance capabilities and defining policy that support the warfighting and garrison communications functions for the Marine Corps.

Specifically, C4 is responsible for policy oversight of information systems standards, information systems integration, both internal and external, to the Marine Corps, and monitoring C4 systems development, DoD, national, and allied systems that impact on the Marine Corps Information Technology architecture, corporate enterprise network applications, Identity Management (IDM), Public Key Infrastructure (PKI), and Information Assurance (IA).

Within C4, the Marine Corps Cyberspace Operations Group (MCCOG), located at Marine Corps Base (MCB), Quantico, Virginia is the Marine Corps implementer of that policy and provides technical expertise, personnel, logistics, management, and facilities necessary to maintain the critical world-wide communications services, operations services, and other services in support of all systems used to communicate data across the Marine Corps Enterprise. The MCCOG maintains a secure, heterogeneous, multi-tiered network in support of classified and unclassified information exchange

requirements. This network provides connectivity for information transmission and sharing between messaging communications servers, clients, TCP/IP hosts and clients in tactical, aboard ship, base, camp, post or station environments. The MCCOG, as the lead operational command within C4, has been tasked with providing for the security and assurance of information exchanged across the Internet and intranets by operating a common interoperable infrastructure based on mandated DoD PKI requirements, biometrics, and complementary technologies in order to enable security services at multiple levels of assurance. The MCCOG receives these material solutions from Marine Corps Systems Command and joint programs of record and also provides fielding and post-deployment support.

Information systems that are vital to the Marine Corps' ability to carry out their mission are targets for our adversaries. HQMC C4, IA Division is tasked the responsibility to coordinate USMC-wide efforts to safeguard the network from attack and preserve our ability to provide reliable and effective network services. Policy for IA implementation rests with HQMC C4. The focus of IA in the Marine Corps is to ensure policies and procedures are implemented, to guarantee assured information delivery, assured data integrity, and assured information protection.

C4, IA Division must direct, oversee, and implement IA policy on all IT resources procured, developed, operated, maintained, or managed throughout the Marine Corps; defend the Marine Corps Enterprise through a defense-in-depth strategy that leverages the capabilities of the MCCOG and the Marine Corps Enterprise Network (MCEN) to achieve strong, effective, multidimensional protection of our IT environment.

2.2 OBJECTIVES

The objective of this performance work statement is to describe the required contractor efforts needed for operational support to USMC PKI programs. Specific objectives are listed below:

- Post-deployment applications software PKI support
- Certificate validation support
- Registration Authority operations
- Integration Support for fielded systems
- Field technical support

2.3 SCOPE

The MCCOG requires support for technical requirements definition, operations and sustainment of Public Key Infrastructure (PKI) and related programs. Contractor support shall include PKI registration support for authorized systems and personnel located at Marine Corps installations worldwide.

Required support includes sustainment of the Marine Corps portion of the established DoD Baseline PKI and support required to achieve the objectives of DoD Increment 2. PKI Increment 2 contains four defined elements: SIPRNet implementation, extension of PKI Services into the Joint Tactical Remote Environment, HSPD-12 requirements and Enhanced Status Quo.

2.4 TASKS

The tasks identified below, when integrated, shall provide the USMC with an effective capability to

execute MCEN IT services. These tasks enable the MCCOG to fulfill its role within the Department of Defense's operational hierarchy, quickly adapting to near-term changes and continuously evolving to meet long-range technology trends.

NOTE: The tasks identified in this PWS are non-personal in nature; therefore, the Contractor's employees are not subject to the supervision and control of the Federal Government employees. All tasks listed below shall be completed in accordance with the PWS and the identified SOP's, and managed by the Contractor with surveillance by the Government. The Contractor shall perform all tasks requiring development in coordination with the MCCOG. The Government will monitor the Contractor's performance to ensure compliance with the PWS and other terms and conditions in accordance with the Government's Quality Assurance Surveillance Plan (QASP) and Performance Requirements Summary (PRS).

Unless otherwise supplemented or superseded, Directives applicable to the performance of the subject work are as follows:

- Information Technology Infrastructure Library (ITIL) version 3 framework established guidelines for the Information Technology Service Management (ITSM) discipline for managing information technology (IT) systems.
- Department of Defense Directive 8570-1 (DoDD 8570-1) - Information Assurance. Training, Certification, and Workforce Management. 12-2005 with Incorporated change of 4-20-2010.
- MARINE CORPS ORDER (MCO) 5510.18A- United States Marine Corps Information and Personnel Security Program Manual
- Secretary of the Navy-SECNAVINST 5510.30B- Department of the Navy (DON) Personnel Security Program (PSP) Instruction
- Secretary of the Navy (SECNAV M-5510.30)--Department of the Navy Personnel Security Program
- Secretary of the Navy (SECNAVINST) 5510.36A- Department of the Navy (DON) Information Security Program (ISP) Instruction
- Secretary of Navy (SECNAV) M-5510.36-Department of the Navy Information Security Program Manual, 1 Jul 06
- Marine Corps Base Order (MCBO) 5510.1C- Information and Personnel Security Program (IPSP)
- Marine Administrative Message (MARADMINs) and United States Marine Corps (USMC) Operational Directives as tasked
- Marine Corps Network Operations and Security Center (MCCOG) policies, procedures and Standard Operating Procedures (SOP)
- Additional Regulatory Guidance: The Contractor shall apply, as appropriate, Marine Corps, Department of the Navy and the Department of Defense Information Assurance policies, procedures, and technical communication requirements as defined under the following, which can be found through the Defense Information Systems Agency (DISA) portal at iase.disa.mil, and United States Cyber Command, <https://www.cybercom.mil/default.aspx>, under the orders and Directives tab.

2.4.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The Contractor shall utilize relevant experience and expertise to provide program management support under this Contract. This includes the management and oversight of all activities performed by Contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The Contractor shall identify a Program Manager (PM), by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this

Contract. The Contractor shall schedule meetings and provide deliverables. The PM shall serve as the Government's primary point-of-contact and provide technical supervision and guidance for all Contractor personnel assigned to support the MCCOG.

The PM shall possess the following knowledge and/or experience:

- Understanding of operational and technical requirements of the MCCOG.
- Understanding of application and network systems similar to those operated by MCCOG.
- Managerial experience in a C4 environment directing technical staff members.
- Excellent written and verbal communication skills, and have demonstrated ability to present material to senior DoD and non-DoD officials.
- C4 experience in a military headquarters or command center environment.

The PM shall possess the following qualifications (qualifications, for the purpose of this PWS, refers to all clearance, certification, experience, and 8570 compliance level as stated in the "Qualification Table" under each task area):

Task 1 - Qualification Table							
Billet Function	Task Area	Clearance	Preferred Tech Certification & Education	Minimum Tech Certification & Education	*Minimum Experience in Relevant Billet Function	8570 Requirements	**Estimated Percentage Augmentation Required
Program Manager (Key Personnel (KP))	2.4.1	Top Secret	*Professional level technical certification (e.g. CCNP or MCITP)	Bachelor's degree in a management related field *Project Management Professional (PMP) certification	10 Years General PM experience and demonstrated IT Related Project or Program Management Experience	IASAE II	100%

*Experience shall be recent, having occurred within the last three years. For example: 5 years of experience required having occurred within the last 7 years. This note applies to all "Qualification Tables" in this PWS.

**The "Estimated Percentage Augmentation Required" column of each Contractor personnel qualification table identifies the approximate level of contractor support that the Contractor shall provide under this contract. These percentages are based on the overall level of effort (Government and Contractor) required to support the size and scope of the MCCOG Network Architecture as identified in section C.3 of this PWS. For example, 50% estimated augmentation for a task requires the Contractor to provide approximately 50% of the overall support services required to successfully perform the task based on the MCCOG Network Architecture and the specifics of the task as identified in this PWS. This note applies to all "Qualification Tables" in this PWS.

2.4.1.1 Monthly Status Report (MSR)

The Contractor PM shall develop and provide a MSR using Microsoft (MS) Office Suite applications or other MCCOG approved application, by the tenth of each month via electronic mail to the

Technical Point of Contact (TPOC) and the COR. The format of the MSR must be submitted to the COR for approval. The MSR shall include the following:

- ☐ Activities during reporting period, i.e. previous month, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- ☐ Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- ☐ Personnel gains, losses, and status (security clearance, etc.).
- ☐ Government actions required.
- ☐ Correlation of operational work performed within S3/S6 to TT and Change Request completion.
- ☐ Correlation of engineering and integration work performed to Project Tasks.
- ☐ Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- ☐ Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).
- ☐ Accumulated invoiced cost for each CLIN up to the previous month.
- ☐ Projected cost of each CLIN for the current month.
- ☐ 8570 Compliance status report (electronically) for each person supporting this contract. This report shall, at a minimum, include for each person: first and last name, job title, required 8570 compliance level, current 8570 level. The MCCOG may ask for electronic copies of certifications as verification that 8570 compliance has been met.

2.4.1.2 Meeting Minutes

The Contractor shall prepare and deliver Meeting and Review Minutes for all formal meetings and reviews. An estimated total of 60 formal meetings per year. Notes shall be provided to the Government for concurrence within 24 hours of meeting. At a minimum the minutes shall contain the following:

- ☐ Date and place
- ☐ Attendees
- ☐ Purpose of meeting/review
- ☐ Brief description of items discussed
- ☐ Results
- ☐ Action items

2.4.1.3 Performance Evaluation/Technical Status Meetings

The Contractor PM shall attend a monthly Contract Activity and Status Meeting with the TPOC, COR, and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. One day prior to the meeting, the Contractor shall provide the COR with an agenda of the meeting. Within three workdays following the meeting the Contractor PM shall provide written minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR. Any non-concurrence of the meeting notes content by the Government Contractor will be provided to the Contractor for revision within three calendar days following receipt of the minutes. The Contractor shall make the necessary changes and provide them to the Government within two workdays.

The Contractor shall prepare a Plan of Action Report for the MCCOG TPOC at the end of each week that presents major weekly Contract activities completed and events and milestones to be completed the following week.

2.4.1.4 Trip Reports

The Contractor shall keep a detailed summary of all travel including, but not limited to, the name of the employee, location of travel, duration of trip, the cost of travel, and point of contact (POC) at travel location. Each month, at the Contract Activity and Status Meeting with the COR, the Contractor shall provide the trip report for the previous month.

2.4.1.5 Project Management Plan (PMP)

The Contractor shall document all support requirements in a PMP. The Contractor shall provide a draft PMP to the Government at the kick-off meeting. The draft PMP is subject to changes pending Government comments and recommendations after the kick-off meeting. The final PMP shall be approved by the COR.

The PMP is an evolutionary document that shall be updated annually, or as directed by the Contracting Officer. The Contractor shall work from the latest Government-approved version of the PMP.

The PMP shall:

- ☐ Describe the proposed management approach
- ☐ Contain detailed Standard Operating Procedures (SOPs) for all tasks
- ☐ Include milestones, tasks, and subtasks required in this Contract
- ☐ Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between or among Government organizations
- ☐ Include the Contractor's QMP (see, C.5.1.6).

2.4.1.6 Quality Management Plan (QMP)

The Contractor shall document its QMP. The Contractor shall provide a draft QMP to the Government at the kick-off meeting. The draft QMP is subject to changes pending Government comments and recommendations after the kick-off meeting. The Contractor shall provide the final QMP within 30 calendar days after Contract award. The final QMP shall be approved by the COR. The Contractor shall periodically update the QMP as changes in program processes are identified.

The QMP shall address the Contractor's plan to meet quality and performance standards outlined in the Quality Assurance Surveillance Plan (QASP) and the Performance Requirements Summary (PRS) and shall include, at a minimum, the following components:

- ☐ Quality objectives
- ☐ Key project deliverables and processes to be reviewed for satisfactory quality level
- ☐ Quality standards
- ☐ Quality control and assurance activities
- ☐ Quality roles and responsibilities
- ☐ Quality tools
- ☐ Plan for reporting quality control and assurance problems

2.4.1.7 Transition-In

The Contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition into this contract. Upon contract award, the Contractor, in coordination with the Government and the incumbent contractor, shall provide phase-in support days beginning at the start of contract performance for up to sixty (60) days thereafter. All transition activities shall be completed no later than 60 calendar days after the start date of the contract. The Contractor shall submit a draft Transition Plan at the Project Kick-Off Meeting. The draft Transition-in Plan is subject to changes pending Government comments and recommendations after the kick-off meeting. The final Transition-In Plan shall be approved by the COR.

The phase-in activities shall include such functions as:

- * Receive knowledge, experience, and lessons learned from incumbent contractor and Government personnel.
- * Assist in startup to ensure no service disruption to MCCOG and a smooth transition.
- * Receive appropriate property, documentation, or personnel, as agreed to between the parties (including but not limited to, devices, equipment, databases and systems related to this PWS).
- * Attend program reviews and participate in working groups, briefings.

The Transition-In Plan shall, at minimum, address the above phase-in activities. The plan shall also include a training program for contractor personnel and a date for accepting responsibilities for each division of work described in the Transition-In Plan. Additionally, proposed staff levels with a work breakdown structure (WBS) during and after the transition in period shall be included within the Transition-In Plan.

2.4.1.8 Transition-Out

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from this Contractor to any subsequent incoming contractor and Government personnel at the expiration of this Contract. The Contractor shall provide a Transition-Out Plan NLT 90 calendar days prior to expiration of this Contract. The Contractor shall identify how it will coordinate with any subsequent incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- ☐ Project management processes
- ☐ Points of contact
- ☐ Location of technical and project management documentation
- ☐ Status of ongoing technical initiatives
- ☐ Appropriate contractor-to-contractor coordination to ensure a seamless transition.
- ☐ Transition of Key Personnel
- ☐ Schedules and milestones
- ☐ Actions required of the Government
- ☐ Submit a "turnover binder" for each functional area which shall include, but is not limited to, passwords, permissions, SOPs, documentation, etc.

The Contractor shall establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

The Contractor shall complete or perform transfer of all tangible and intangible (intellectual) property and licenses.

The Contractor shall implement its Transition-Out Plan no later than 75 calendar days prior to expiration of the contract.

2.4.1.9 Program Kick-Off Meeting

The Contractor shall schedule and coordinate a Program Kick-Off Meeting to occur within 10 working days after Contract award at the Government's primary site at Quantico Marine Corps Base. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with this Contract. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include vital contractor personnel, representatives from the directorates, other relevant Government personnel, and the Contracting Officer's Representative (COR). The Contractor shall provide the following at the Kick-Off Meeting:

- ☐ Draft Transition-In Plan
- ☐ Draft Project Management Plan
- ☐ Draft Quality Management Plan (QMP)

2.4.1.10 Training Space

The Contractor shall make available to the MCCOG, as needed and within 14 days of request by the MCCOG, a secure space in a classroom or conference room configuration to conduct training for approximately 10-20 students per session. The Contractor shall provide audio/visual support to include an overhead projector and screen, and internet connectivity which allows vendors to reach back to their network servers or sites as required to provide the course. The physical training space shall be located within 25 miles of the MCCOG facility, Quantico, VA.

2.4.2 TASK 2 – PROVIDE PUBLIC KEY INFRASTRUCTURE SUPPORT (MCCOGS3)

The mission of the USMC Public Key Infrastructure (PKI) Program provides the resources, manpower and equipment (hardware and software), dedicated to the management (i.e.: generation, production, distribution, control, accounting and destruction) of keys and certificates used by public key-based security services to include NIPRNet and SIPRNet both garrison and deployed. The PKI program operates the USMC Certificate Validation Infrastructure necessary to ensure that only authorized users and server based applications are allowed to operate on the Marine Corps Enterprise Network (MCEN). These services are required for user access to all information system components on the MCEN including network accounts, applications and web sites. PKI must be operable in garrison and tactical/deployed environments.

The Contractor shall possess the following qualifications:

Task 2 – Qualification

Billet Function	Task	Clearance	Minimum Tech Certification & Education	*Minimum Experience in Relevant Billet	8570 Requirements	**Estimated Percentage Augmentation Required
Registration Authority (KP)	2.4.2.1	Secret	Technical Series Certification Security+ CE Key Recovery Registration Authority Certification CRR Reset	2 years	IAM 1	75%
Implementation Planner	2.4.2.2	Secret	Technical Series Certification Security+ CE ITILv3	4 years	IAM 1	75%

Task 2 – Qualification Table						
Billet Function	Task	Clearance	Minimum Tech Certification & Education	*Minimum Experience in Relevant Billet Functions	8570 Requirements	**Estimated Percentage Augmentation Required
Local Registration Authority	2.4.2.3	Secret	Technical Series Certification Security+ CE Local Registration Authority CertificationCPR Reset ITILv3 Foundations	2 years	IAM 1	100%
Network Operations	2.4.2.4 2.4.2.5 2.4.2.6	Secret	Technical Series Certification MCSA 2008 Security+ CE	4 years 2 years (PKI)	IAT 2	100%
Network Operations Senior	2.4.2.4 2.4.2.5 2.4.2.6 2.4.2.7	Secret	Technical Series Certification MCSA 2008 Security+ CE Axway Associate Level Certification	8 years 4 years (PKI)	IAT 2	100%
Network Operations Lead (KP)	2.4.2.4 2.4.2.5	Top Secret (SCI eligibility)	MCSE 2008 CISSP Axway Associates-level certification	10 years 7 years (PKI)	IAT 3	75%
Programmer/ Database Administrator	2.4.2.7	Secret	Security+ CE	8 Years 3 Years (PKI)	IAT 2	100%
Information Assurance Compliance	2.4.2.8	Secret	MCSA 2008 SCCVI/ACAS HBSS 201 MCCAST Security+ CE	8 years	IAT 2	75%

The Contactor shall assist in providing PKI support services under the following subtasks.

2.4.2.1 Registration Authority (RA) Operations

The Contractor shall provide PKI RA support for the implementation, maintenance and up keep of the DoD/NSS/USMC Public Key Infrastructures by the creation and removal of LRAs, the issuance and revocation of Role Based, Code Signing, End user, administrator and server certificates, Alternate token issuance, certificate suspension, key recovery, SIPRNet Token and CAC PIN resets. The Contractor shall manage the production and issuance of USMC Alternate Tokens using the USMC Card Management System and production and issuance of the DoD/NSS SIPRNet tokens using the Token Management System (TMS). The PKI RA section is a fast paced work environment and serves

as the only PKI Enterprise help desk in the USMC providing professional and courteous support to customers located throughout the world to include tactical environments. The Contractor will be required to use PKI RA and customer service skills to enhance the network security by the use of PKI while working with internal MCCOG divisions, external Marine Corps organizations, various other Department of Defense organizations and a myriad of Government and civilian organizations to provide the following:

- Certificate issuance/Revocation
- Help Desk Support
- CAC Pin Reset Support
- PKI Key Recovery

Directives applicable to the performance of the subject work are as follows:

- United States Department of Defense X.509 Certificate Policy, Version 10.5, 23 January 2013.
- Department of Defense Instruction: 8500.2, Information Assurance (IA) Implementation, 06 Feb 2003
- Department of Defense Instruction: 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011
- USMC Medium Assurance PKI RA/LRA Certification Practice Statement, 25 July 2012
- CNSS Instruction No. 1300 (Instruction for National Security Systems PKI X.509 CP Under CNSS Policy No. 25), SEP 18, 2013
- National Security Systems PKI - Department of Defense Registration Practice Statement, V6, 22 MAY 2013

The Contractor shall identify support personnel to serve as the RA staff assigned under this subtask area and possess a DoD/NSS PKI certification as a DoD/NSS Registration Authority (RA) and must be a U.S. Citizen. The Contractor shall use its direct DoD/NSS PKI experience to provide the following RA operations support:

- Serve as RAs and Key Recovery Agents.
- Maintain support for creation and removal of LRAs.
- Issue end user certificates. Perform installation of X.509 certificates on to Blackberry devices
- Execute certificate revocation within 12 hours of notification.
- Download, format, and install PKI certificates.
- Common Access Card (CAC) PIN Reset and Key recovery.
- SIPR Token PIN Reset and Key recovery.
- Resolve customer issues related to PKI certificate use and system configuration.
- Serve as the Liaison between the MCCOG and the field LRA staff for the resolution of issues elevated to the MCCOG call center.
- Submit and update Remedy tickets in accordance with established metrics.
- Execute certificate disposition for USMC casualties.
- Assist in the execution of LRA and end user PKI training.
- Manage the production and issuance of DoD SIPR Tokens using a Token Management System and peripherals provided by the Government at the

MCCOG. Required production rates are expected to be such that in excess of 5,000 tokens must be produced in the first year of the period of performance, and may increase thereafter.

- Manage the production and issuance of USMC Alternate PKI Tokens using a Card Management System and peripherals provided by the Government at the MCCOG.
- Maintain and sustain the central repository of PKI records specified by the Government, to include records required to establish the validity of a signature and the proper operation of the PKI as specified in the DoD PKI Certificate Policy. Paper copies of DD Form 2841 and DD Form 2842 must be manually scanned and marked with identifying data elements required for retrieval by automated search.
- Perform metric collection and reporting on selected activities directed by the Government. The Contractor shall maintain a daily log of user assistance calls, SIPR token and Alternate token certificate issuance, revocations and server certificate issuance to be incorporated into the a monthly status report.
- Each Contractor shall maintain a daily physical logbook consisting of all RA certificate activities as specified in the DoD RA CPS/NSS RPS.
- Maintain and update required PKI certificate issuance, revocation, and key recover actions in appropriate existing or future SharePoint lists/Databases.
- Provide data requirements for future SharePoint lists/databases for issuance activities from new DoD capabilities.
- Direct calls from key operators of the DoD and USMC PK Infrastructure to appropriate MCCOG Sections.
- Provide both internal and external USMC PKI customers with knowledgeable, problem-solving resolutions, in the shortest time possible to minimize any customer downtime or work stoppage.
- Assist Program of Record (POR) application owners with integration of current USMC PKI enabling technologies.
- Provide general administrative support tasks to the execution of PKI logistics activities such as controlled distribution of SIPR Tokens, ALT Tokens, and PKI peripherals.
- Provide input for operational metrics and analysis to improve the enterprise PKI related customer experience and reduce Help Desk calls.
- Provide desktop and network support.
- Perform operational testing of beta tokens, new certificate types and Token Management Testing along with operational capability testing of all new versions of PKI certificate and systems.
- Excellent written and verbal communication skills required.

2.4.2.2 Implementation and Planning

The Contractor shall provide implementation and planning support in the development and writing of project plans and implementation documentation as required in support of USMC PKI initiatives. This also includes updating existing specific PKI plans and procedures to comply with changing DoD PKI initiatives. Development of plans for the employment and support of PKI tools in all network environments to include tactical which provides PKI procedures for concept of operations (CONOPS) and plan of actions and milestones (POA&M) to ensure successful execution.

- a. The Contractor shall identify support personnel to serve as the Implementation and planning staff assigned under this subtask area and shall use direct DoD PKI experience, and communication and presentation skills to provide the following services: Web Page/ SharePoint Administrator

USMC PKI manages and maintains an internal and external Sharepoint site which provides internal collaboration and external customer support services. Internal support services includes but not limited

to document libraries, task tracking, calendar, database and list services. External customer support services include, but are not limited to, PK Enabling documentation, Software configurations, and downloads.

The Contractor shall use its direct SharePoint experience and skills to:

- Create, maintain, and sustain document libraries and lists.
- Create, maintain, and sustain views for libraries and lists.
- Create, maintain, and sustain WebParts as necessary.
- Create, maintain, and sustain templates for assisting PKI Personnel with individual document libraries.
- Provide access to PKI information utilizing Excel Web Services.
- Create, maintain, and sustain Key Performance Indicator (KPI) web parts.
- Connect web parts.
- Create individual web pages to simulate “collaborative sites”.
- Employ web services to present information from restricted areas to the general public.
- Write basic scripts (e.g., providing Site Redirection, adding color to a list item in SharePoint, etc.).
- Set proper security settings and permissions.
- Maintain, sustain, and update 5 SharePoint lists for the tracking of SIPRNet Trusted Agents (775), NIPRNet Trusted Agents (407), Alternate Tokens (3076), SIPRNet Tokens (38351) and Server Certificates (6295). *Numbers in parenthesis indicate current database line items*
- Develop and maintain additional share point lists as required.
- Develop required reporting from SharePoint Lists using available tools.
- Develop, maintain, and sustain the external PKI SharePoint content as required by Government leadership.

b. LRA Auditor

The Contractor shall use its direct DoD PKI experience and excellent communications and presentation skills to provide LRA Audit support for the development, updating and execution of comprehensive audit procedures and reports for all LRA field operations. The Contractor shall have all travel approved by the MCCOG TPOC and COR in advance, which may require passport for OCONUS travel.

The Contractor shall use its business system analysis experience and skills to:

- Develop, modify, and execute comprehensive audit procedures for all LRA field operations.
- Conduct and ensure performance of field LRA operations audits are in accordance with the most current USMC LRA Certificate Practice Statements (CPS), (Committee National Security System (CNSS) Certificate Policy (CP) the USMC Training User’s Guide, and USMC RA guidance
- Maintain all procedures, reports, and Naval messages to ensure the USMC RA maintains a prepared state for the successful completion of the LRA audits directed by the DoD CPS and NSS RPS.
- Draft and submit LRA Audit reports within 30 days of audit completion for signature and delivery to audited Command
- Recommend improvements to procedures and processes related to the audits to PKI Leadership

- Excellent written and verbal communication skills

The Contractor shall plan for two personnel for each audit taking one week at the following locations:

- Camp Lejeune, NC
- Camp Pendleton, CA
- Okinawa, Japan
- Stuttgart, Germany

c. Program of Record (POR) PKE Waiver Review

The Contractor shall provide implementation and planning support for reviewing USMC POR Application waiver forms for compliance/noncompliance with existing DoD PKI directives. Due to technical limitations, some systems are unable to implement PKI and therefore require a waiver form to justify non-compliance with PKI directives..

The Contractor shall use Business Analysis and direct DoD PKI experience to:

- Review and submit waiver forms with recommendation for approve/disapproval to the USMC DAA/AO
- Create, submit, and track Remedy trouble ticket for waiver requests
- Track all waiver forms using SharePoint and notify the POR requestor of waiver status
- Coordinate directly with the USMC PKI Network Operations for technical guidance to verify requested waiver system is capable or incapable of PK enablement.
- Develop, maintain, and provide briefings to Government leadership depicting current status of waived systems/PORs.
- Excellent written and verbal communication skills required

d. General Officer(GO)/ Senior Executive Service(SES) Blackberry Support

The Contractor shall provide Implementation and Planning support for updating and configuration of USMC GO and SES members with the installation of PKI software certificates onto their Blackberry devices, allowing them to access signed and encrypted e-mails without the use of a Common Access Card (CAC) sled. The Contractor will be required to travel (local) and coordinate directly with GO/SES staff and may occasionally interact directly with GO/SES. The Contractor shall maintain a professional/mature demeanor and dress accordingly during any interactions with GO/SES and/or their staff. The Contractor shall anticipate complications and coordinate support staff in order to minimize disruption/inconvenience to the GO/SES.

The Contractor shall use direct DoD PKI and Blackberry experience and knowledge to provide the following services to support PKI implementation planning support for the following General Officer Blackberry Support:

- Coordinate with GO/SES staff for the implementation of Blackberry certificates.
- Coordinate with other MCCOG sections (EDM/S6) for proper configuration of Blackberry device and network support.
- Perform initial Blackberry troubleshooting of signing and encrypting emails
- Provide initial Blackberry Desktop Manager support
- Develop and maintain POA&M for yearly GO Symposium and/or GO/SES conferences and provide onsite support.
- Develop, maintain and provide power point presentations upon completion of

GO/SES Symposium support.

- Establish and execute SOPs to ensure version control and adherence to sound configuration management practices for all documentation.
- Submit/update/close Remedy trouble ticket
- Installations may require travelling to the GO/SES location and coordinating the logistics with GO/SES staff.
- Excellent written and verbal communication skills

e. Concept of Operations (CONOPS)/Operational Directives/Advisories (OPDIR/OPAD) Development, Tracking and Reporting

The Contractor shall use direct business process consultant experience and technical writing skills to:

- Perform technical writing, analysis, and editing of all PKI CONOPS with technical SME assistance
- Develop, review, and release OPDIR/OPAD in accordance with Government leadership guidance for release of operational requirements and advisories. Provide reporting guidance and/or templates as required.
- Track and report OPDIR compliancy from reporting commands and create reports for briefings to leadership
- Contact non-compliant commands and report to Government leadership with the status.

f. USMC and DoD PKI Document/Meeting Review

The Contractor shall use Business Process Consultant and DoD PKI experience to support PKI implementation and planning for the following meetings (weekly/biweekly/monthly):

- DoD PKI Program Management Office (DoD PKI PMO) meeting
- Identity Protection and Management Senior Coordinating Group (IPMSCG) meeting and meetings of IPMSCG sub-groups
- Non-person Entity Process Action Team (NPE PAT)
- DoD PKI Technical Interchange meeting
- USMC PKI and Identity Management programs
- SIPRNet Process Action Team Meetings
- SIPRNet WIPT meetings
- SIPRNet requirements meetings
- DCCB meetings
- Other meetings as required

The Contractor shall use input from these meetings and provide the following PKI implementation planning support to:

- Develop USMC PKI Plans and Implementation Documentation for new DoD / USMC projects, tasks, and initiatives. Review and provide comments on plans and procedures of changes to existing DoD and USMC PKI programs and update USMC-specific Plans and Procedures to comply with approved changes to DoD PKI initiatives.
- Develop PKI Tactical Plans for the deployment and support of PKI in tactical environments which shall include Concept of Operation Plans, Implementation Plans, Continuity of Operations Plans, and Standard Operating Procedures.
- Develop and maintain all PKI Architecture and migration Plans (to include but not limited to: technical, certificate authority, certificate validation, and registration authority) for future releases of DoD PKI.

- Provide analysis, planning, implementation support to assist PKI Section with tasks and requirements levied by USCYBERCOM, MARFORCYBER.
- Review and provide recommendations for or PKI policy and procedures at the DoD, DON, and USMC levels.
- Review and recommend PKI solutions to customer problems based on an understanding of the customer environment and provide recommendations to support the customer's mission.

g. Remedy/Task Tracking

USMC PKI implementation and planning is responsible for coordinating activities to resolve Incidents/Service Requests and restore service with a primary focus on workforce monitoring, prioritization, Incident routing, and queue management.

Tasks/projects external to incident management are created and tracked using SharePoint Tasks Lists.

The Contractor shall use its Business Systems Analyst knowledge and experience of trouble ticketing tools (e.g., BMC Remedy) and SharePoint Tasks Lists and to provide customer service using effective communication best practices to:

- Assign Incidents to and manage the Incident resolution efforts of the Subject Matter Experts (SMEs) to ensure metric compliance IAW established ticketing procedures.
- Ensure Incidents/Service Requests are accurately transferred to appropriate Queues and/or escalated to the proper functional group within prescribed standards and timelines.
- Monitor the performance and investigate/remediate Service Level breaches.
- Ensure Incidents/Service Requests are properly documented to include priority based on impact/urgency, classification, complete and thorough updates at an appropriate level of detail on resolution.
- Create and manage tasks using SharePoint Task lists.
- Monitor and investigate tasks to ensure timely completion by assigned due date.
- Analyze tasks to ensure proper updates prior to reporting to leadership.

h. Training Documentation Support

The Contractor shall conduct training and outreach activities in support of Marine Corps PKI initiatives for Garrison and Tactical Networks. This includes training plans, activities, developing and maintaining training material, tracking and reporting training activities, supporting PKI computer based training for target audiences as requested, developing and maintaining outreach activities to support PKI and related implementation changes from Joint/USMC programs. The Contractor shall develop, prepare, and train PKI RA, LRA and TA (Trusted Agent) and others as directed via formal classroom courses, workshops and seminars. Training shall be in conformance to Information Assurance policy

The Contractor shall use its business systems analyst knowledge and experience of DoD PKI and training/outreach support to:

- Develop PKI Training Plans and tactical training materials.
- Develop and maintain tracking and reporting mechanisms for tactical training suite and materials.
- Report physical location of tactical training suite and materials during shipment, ensuring timely arrival at training location.

- Develop and maintain PKI Outreach Materials to support PKI training and customer awareness as related to constant changing of PKI environment.
- Develop and provide PKI Briefs for conferences or working group meetings regarding PKI projects, plans, and initiatives as directed. Develop and provide targeted computer/hands-on training specific to Local Registration Authorities, system administrators, and end-users within USMC, to include the DoD PKI Conferences.
- Develop and provide PKI Instructor Materials such as course outlines, background material, and training aids in support of targeted training.
- Develop and provide PKI student course materials such as workbooks, handouts, completion certificates, and course critique forms for onsite hands-on training.
- The Contractor shall train PKI LRAs in accordance with the USMC, DISA, and NSA IA policy and procedures via formal classroom courses, and hands-on workshops.

2.4.2.3 Local Registration Authorities (LRAs)

The Contractor shall provide Local Registration Authority (LRA) support at each MEF location and MARFOREUR to assist in G6 PKI mission. The Contractor LRA shall assist in all PKI implementations, server builds and installs in conjunction with the Local G6's.

The Contractor shall identify support personnel to serve as the LRA staff assigned under this subtask area and possess a DoD/NSS PKI certification as a DoD/NSS Local Registration Authority (LRA) and must be a U.S. Citizen.

The Contractor shall use its direct DoD/NSS PKI experience to:

- Provide Local Registration Authority (LRA) support to ensure the PKI Server Certificates are requested, approved, and installed IAW PKI Policy. Provide PKI end-user training on certificate utilization within the Desktop environment.
- Maintain and perform CAC PIN Reset operations for end-user needs in area of responsibility(AOR)
- Execute PKI certificate registration, management and revocation requests to ensure all requests activities are properly documented within ticket management system.
- Archive PKI data as directed and in compliance with the CPS/RPS Plan, coordinate, and implement, at the local level with the local G6, evolving PKI initiatives as directed by the USMC RA..
- The Contractor LRA located at Camp Pendleton is designated as the COOP RA for the USMC. In the event of operational transfer to the alternate site the Contractor LRA shall address all actions in subtask 3.1 (RA Operations). Required DoD RA training will be conducted at a designated DISA location. Develop, update and submit Weekly and Monthly status reports providing token issuance numbers, trouble calls processed and any current issues to MCCOG Det Lead and USMC RA.

2.4.2.4 PKI Network Operations

PKI Network Operations provides technical expertise related to the support of concept exploration functional and technical requirements generation, development, implementation and enhancement of DoD PK Infrastructure for the Marine Corps. This technical support includes the development of a technically resilient certificate revocation status checking infrastructure for all MCEN networks, as well as meeting the requirements of HSPD-12. It ensures that USMC PKI implementation requirements are identified and made part of the development, implementation and support of the DoD PKI Increment 2 architecture. MCCOG PKI provides support for assessments of USMC impacts from actions associated with DoD PKI PMO development and implementation activities, to include use of DoD PKI with mobile

devices and DoD provided non-person entity issuance capabilities. As well as provide support to address issues related to certificates, tokens, token issuance, and infrastructure services. This task provides technical requirement support to directory service providers and recommendations for USMC action to change DoD implementation and software releases. USMC PKI recommendations shall also include the impact of planned changes to registration software and hardware upon USMC users.

The Contractor shall identify support personnel to serve as the PKI Network Operations staff assigned under this subtask area.

The Contractor shall identify support personnel to serve as the PKI Network Operations Network Operations Lead which provides technical supervision and guidance for all PKI NetOps system management tasks supporting the MCCOG. The PKI NetOps Network Operations Lead should be able to demonstrate the following knowledge and/or experience:

- In depth experience providing Tier III or higher support for PKI services
- Expert knowledge of PKI and collaboration technologies similar to those in use by the USMC
- Substantial experience operating and maintaining Certificate Authorities and Certificate validation infrastructures.
- System design and engineering experience with focused experience developing and implementing PKI system's similar to those maintained and delivered by the MCCOG
- Excellent written and verbal communication skills, and have experience effectively presenting material to senior DoD and non-DoD officials
- Managerial experience in a C4 environment directing 10 or more technical staff members.
- Experience evaluating and implementing emerging industry-standard PKI Technologies
- Experience incorporating emerging technologies into existing environments

a. Certificate Authority(CA) Support

The Contractor shall use its active directory experience, direct DoD PKI experience, Unix and Windows software, Microsoft and Red Hat CA software knowledge and experience to provide CA support:

The Contractor shall:

- Develop, deploy and configure new CA Infrastructure
- Conduct infrastructure checks twice daily and create status report using SharePoint List for Government leadership.
- Maintain the overall health of technologies associated with the CA infrastructure.
- Monitor the health of CA infrastructure with MCCOG provided event management tools. Report any discrepancies to Government leadership and record using incident ticketing system.
- Publish and issue Certificate Revocation Lists on a weekly basis from Offline and Sub CAs.
- Provide Tier III troubleshooting and support for incidents related to CAs and document resolution using incident ticketing system.
- Implement and monitor CA thresholds and conduct proactive event remediation per Government guidance.
- Develop, plan, deploy, and configure new versions of CA Infrastructure as needed or when directed by Government leadership.
- Develop, test, and maintain CA Infrastructure disaster recovery plans using

SharePoint Document Library. .

- Develop, test, and maintain CA Infrastructure COOP plans using SharePoint Document Library.
- Escalate issues to third party product vendors as required and track the progress of vendor support.

b. Certificate Validation Infrastructure (CVI) Support

The Contractor shall use its PKI, Windows Software knowledge, and Axway Validation Authority Suite software to include but not limited to OSCP, Desktop Validator, Enterprise Validation Authority, and Compact CRLs experience to provide CVI support.

The Contractor shall:

- Configure and deploy new Certificate Validation (Responder/Repeater) software as needed or directed by Government leadership.
- Develop, deploy and maintain desktop validator configurations for use by all systems and applications residing on all USMC networks.
- Conduct infrastructure checks twice daily and create status report using SharePoint List for Government leadership.
- Maintain the overall health of technologies associated with the Certificate validation infrastructure.
- Monitor the health of CVI with MCCOG provided event management tools. Report any discrepancies to Government leadership and record using incident ticketing system.
- Ensure validation information, downloaded from DISA, is current and accessible by CVI servers.
- Provide Tier III troubleshooting and support for incidents related to CVI and document resolution using incident ticketing system.
- Configure and deploy new versions of CVI as needed or when directed by Government leadership.
- Develop, test, and maintain CVI disaster recovery plans using SharePoint Document Library.
- Develop, test, and maintain CVI COOP plans using SharePoint Document Library.
- Escalate issues to third party product vendors as required and track the progress of vendor support.

c. Hardware Security Module Support

The Contractor shall use its PKI, Windows software knowledge, and SafeNET and nCipher hardware experience to provide Hardware Security Module (HSM) support to provide PKI certificate services

The Contractor shall:

- Configure and deploy new HSMs as required or directed by Government leadership
- Maintain the overall health of the HSMs. Provide Tier III troubleshooting and support for incidents related to HSMs and document resolution using incident ticketing system.
- Develop, test, and maintain HSM disaster recovery plans using SharePoint

Document Library.

- Escalate issues to third party product vendors as required and track the progress of vendor support.

d. Public Key Enabling Support

The Contractor shall use its network engineering, DoD PKI, Unix experience, and Windows software knowledge, and Online Certificate Status Protocol (OCSP) and experience with active directory structure to assist in providing PK Enabling Support.

The Contractor shall:

- Investigate and understand new technologies that require PK Enablement
- Receive and review PKI noncompliance waiver requests and recommend approval/disapproval to subtask 3.2 (Implementation and Planning)
- Create courses of action and document recommendations for PK Enabling noncompliant systems. POR/Application owners are responsible for Cryptographic Enablement.

e. Tier III Support

The Contractor shall use its network engineering, DoD PKI, Unix experience, and Windows software knowledge, and Online Certificate Status Protocol (OCSP), and experience with active directory structure to assist in providing TIER III Support.

The Contractor shall:

- Perform PKI TIER III troubleshooting on MCEN systems relating to PKI specific incidents to include but not limited to cryptographic logon, certificate validation, and domain controller certificates.
- Participate and provide PKI subject matter expertise in resolving issues within all USMC Networks in collaboration with other MCEN service providers
- Understand entire MCEN architecture and infrastructure and how PKI is integrated from the end user to service delivery points

f. Card Management System (CMS) Support

The Contractor shall use its DoD PKI and ActivIdentity Card Management system experience, to provide Alternate Token management and issuing services.

The Contractor shall:

- Plan, configure and deploy new CMS system.
- Develop, deploy and maintain CMS Structured Query Language (SQL) database system

- Maintain the overall health of technologies associated with the CMS and token management
- Provide Tier III troubleshooting and support for incidents related to CMS and document resolution using incident ticketing system.
- Develop and maintain CMS disaster recovery plan.
- Escalate issues to third party product vendors as required and track the progress of vendor support.

g. Configuration Management Support

The Contractor shall use its Configuration Management system knowledge and DoD PKI experience, to provide Configuration management support.

The Contractor shall:

- Maintain and deploy Desktop Validator and Middleware Configurations supporting the MCEN using SharePoint Document Library.
- Maintain and deploy Server Validator Configurations supporting the MCEN using SharePoint Document Library.
- Maintain baseline configurations for all PKI software and enterprise hardware using SharePoint Document Library.
- Plan, develop, and test, new configurations for PKI software and hardware. Provide after action reports of test results and recommendations for site/region/enterprise implementation
-

The average mean time to resolve tickets per the Watch Officer Key Performance Indicator Policy is listed below:

	Critical (P1)	High (P2)	Medium (P3)	Low (P4)
Assignment to technician/ initialed response	10 Minutes	30 Minutes	60 Minutes	60 Minutes
Updates	90 Minutes	12 Hours	72 Hours	7 Days
Updates at Pending Status	90 Minutes	24 Hours	7 Days, 4 Hours	14 Days
Resolution	8 hours	24 Hours	4 Days/5 Days	7 Days/10 Days

2.4.2.5 PKI System Infrastructure Support

The Contractor shall provide hardware and software technical support to operate, troubleshoot, and scale three separate forests with completely separate infrastructure and services. Each environment requires isolated access, patching, and security postures. The uptime of all PKI enterprise services is 99.97%, not including system maintenance. The Contractor shall identify support personnel to serve as the PKI System Infrastructure Support staff assigned under this subtask area.

The contract shall provide three quotes from different vender sources for new procurement of hardware and software using Government provide requirements.

All patching and Information Assurance Vulnerability Alert compliancy has to be accomplished, with or without a patching solution, on all PKI Enterprise services in accordance with the MCCOG change policy and within a six-day window of guidance. All security vulnerabilities will be remediated and completed within the assigned deadline from C.5.7.8. For vulnerabilities that are technically unable to be remediated, PKI System Infrastructure Tech will assist C.5.7.8 in creating POA&M.

a. Virtual Machine Infrastructure Support

The Contractor shall configure all aspects of the Virtual Infrastructure in support of the PKI Enterprise Services on USMC operated networks. The Contractor shall use its experience with VMware and the experience to deploy and maintain complex VMware environments to provide Virtual Machine services.

The Contractor shall:

- Maintain the overall health of technologies associated with the Virtual Infrastructure (VI).
- Implement monitoring tool thresholds and conduct proactive event remediation as directed by Government leadership.
- Monitor the health of VI with MCCOG provided event management tools. Report any discrepancies to Government leadership and record using incident ticketing system.
- Provide Tier III troubleshooting and support for incidents related to VI and document resolution using incident ticketing system.
- Configure and deploy new versions of VI as needed or when directed by Government leadership.
- Develop, test, and maintain VI disaster recovery plans using SharePoint Document Library.
- Escalate issues to third party product vendors as required and track the progress of vendor support.

b. Storage Area Network(SAN) Support

The Contractor shall configure all aspects of the SAN hardware and software supporting PKI Enterprise Services. The Contractor shall use its experience with NETAPP Storage devices to include Snaps, storage provisioning, management software, recovery procedures, hardware installation and security of Logical Unit Numbers (LUNS) and access to each to provide PKI SAN support.

The Contractor shall:

- Maintain the overall health of technologies associated with the SAN.
- Implement monitoring tool thresholds and conduct proactive event remediation as directed by Government leadership.
- Monitor the health of SAN with MCCOG provided event management tools. Report any discrepancies to Government leadership and record using incident ticketing system.
- Provide Tier III troubleshooting and support for incidents related to SAN and document resolution using incident ticketing system.
- Configure and deploy new versions of SAN as needed or when directed by Government leadership.
- Develop, test, and maintain SAN disaster recovery plans using SharePoint Document Library.
- Escalate issues to third party product vendors as required and track the progress of vendor support.

c. Hardware Load Balancing Support

The Contractor shall use its experience with Network Switching and load balancing equipment to provide PKI networking support service. The Contractor shall use its expertise with Cisco and F5 hardware and support of the products to provide PKI load balancing services.

The Contractor shall:

- Maintain the overall health of technologies associated with the Hardware Load Balancing.
- Implement monitoring tool thresholds and conduct proactive event remediation as directed by Government leadership.
- Monitor the health of Hardware Load Balancing with MCCOG provided event management tools. Report any discrepancies to Government leadership and record using incident ticketing system.
- Provide Tier III troubleshooting and support for incidents related to Hardware Load Balancing and document resolution using incident ticketing system.
- Configure and deploy new versions of Hardware Load Balancing as needed or when directed by Government leadership.
- Develop, test, and maintain Hardware Load Balancing disaster recovery plans using SharePoint Document Library.
- Escalate issues to third party product vendors as required and track the progress of vendor support.

d. Server Management Support

The Contractor shall use its knowledge and experience of the Windows server, UNIX and LINUX operating systems and server hardware.

The Contractor shall:

- Maintain the overall health of technologies associated with the Server Management.
- Implement monitoring tool thresholds and conduct proactive event remediation as directed by Government leadership.
- Monitor the health of Server Management with MCCOG provided event management tools. Report any discrepancies to Government leadership and record using incident ticketing system.
- Provide Tier III troubleshooting and support for incidents related to Server Management and document resolution using incident ticketing system.
- Configure and deploy new versions of Server Management as needed or when directed by Government leadership.
- Develop, test, and maintain Server Management disaster recovery plans using SharePoint Document Library.
- Escalate issues to third party product vendors as required and track the progress of vendor support.

e. Event Management Support

The Contractor shall represent PKI within the USMC provided event manager process for all PKI Enterprise Services. The contractor shall install agents where necessary and configure rules and alerts consistent with the support structure.

The Contractor shall:

- Resolve all PKI related Event Management tickets and provide an Event Management Status Report on weekly basis for all Event Management incidents.
- Submit and execute Event Management related Request for Change (RFC) tasks, when required, with approval of Government leadership.
- Maintain the overall health of technologies associated with Event Management tools installed within PKI Enterprise servers.
- Coordinate and collaborate with S5 and other MCCOG sections on Event Management issues.
- Participate in and brief PKI RFC tasks, related to event management, to the Change Review Board.

- Implement monitoring tool thresholds, analyze, and conduct proactive event remediation as needed.

f. Unified Communications(UC) Support

The Contractor shall use its knowledge and experience of the DoD PKI architecture and policies in order to provide the following PKI support:

- Implement PKI technologies within the MCEN UC environment to include but not limited to VOIP Technologies.
- Collaborate with MCEN UC technicians to assist with developing processes and procedures that will be used to interoperate voice and video technologies with PKI and developing best practices as these technologies are deployed across the MCEN.

2.4.2.6 Tactical PKI Training Support

The USMC PKI tactical training support includes training plans, activities, developing and maintaining training material, tracking and reporting training activities, supporting PKI computer based training for target audiences as requested, developing and maintaining outreach activities to support PKI and related changes from Joint/USMC programs.

The Contractor shall identify support personnel to serve as the PKI Tactical Training Support staff assigned under this subtask area. Contractors will be required to travel to CONUS or OCONUS multiple weeks requiring a passport.

The Contractor shall:

- Conduct hands-on training and outreach activities in support of Marine Corps PKI initiatives, to include, but not limited to:
 - PKI 101
 - Certificate Validation Infrastructure
 - Cryptographic Logon (CLO)
 - Administration and Troubleshooting
 - Hands-on Lab
 - Practical Application testing
 - Written test
- Provide tactical PKI instructor, courseware maintenance and course materials for deploying Marines.
- Assist with PKI Training Plans and tactical training materials in support of 3.2.
- Support target audiences with tailored PKI computer-based training
- Developing and maintaining other PKI Outreach Materials to support PKI and related implementation and changes/fielding's from Joint and USMC programs.
- Configure and maintain PKI Tactical training suite by resetting classroom virtual environment back to baseline configuration for servers and workstations.
- Coordinate dates of training and onsite support with requesting MEFs, MEUs, Reserve Commands.

2.4.2.7 PKI Application/Software Support

USMC PKI utilizes multiple customized tools, programs, and scripts that provide streamlined business processes and technical monitoring for USMC PKI Enterprise services. Requests for new tools and scripts occur frequently which support the USMC PKI overall service to the user community.

The Contractor shall identify support personnel to serve as the PKI App/Software Support staff assigned under this subtask area.

a. RA Database Support

The Contractor shall enhance and maintain the USMC RA Database which provides token issuance logging for quick record lookup and archival purposes. The Contractor shall use its experience with SharePoint database/List to provide RA database support.

The Contractor shall:

- Create and maintain Microsoft SharePoint List and Database in support of RA Operation requirements in tracking token and certificate lifecycle.
- Create and manage of all RA SharePoint lists and databases in support of disaster recovery efforts.
- Develop new enhancements to current SharePoint list database capabilities.

b. CMS Support

The Contractor shall provide database and DoD/DISA CA connector support to enhance and maintain the USMC ActivIdentity Card Management System (CMS) system. The USMC CMS provides card management services and allows for the issuance of Alternate Logon Tokens with the capabilities to reset pins remotely. The Contractor shall use its experience with CMS to provide application support.

The Contractor shall:

- Install, test, and verify CMS DoD/DISA CA Connector functions with new versions of CMS.
- Configure and maintain database connection with CMS and SQL backend servers
- Create custom scripts for CMS in accordance with 3.1 requirements
- Perform SQL database backup on a weekly basis and stored offsite.

c. Script Development

The Contractor shall create and maintain scripts to enhance and streamline PKI processes and services. The Contractor shall use experience and skills with DoD PKI and VBScript, PowerShell, Batch, Java Script, and Perl scripting languages to support USMC PKI Operations.

The Contractor shall:

- Develop, test, and implement new script capabilities as directed by Government Leadership.
- Maintain, validate, and ensure compatibility of existing custom scripts.

d. Application Development

The Contractor shall create and maintain applications to enhance and streamline PKI processes and services. The Contractor shall use its experience and skills with DoD PKI and C, C++, C#, .NET, Java, SQL programming languages to support USMC PKI Operations support.

The Contractor shall:

- Develop, test, and implement new application capabilities as directed by Government Leadership.
- Maintain, validate, and ensure compatibility of existing custom applications.

2.4.2.8 PKI Information Assurance Support

The contractor shall ensure compliance with all DoD Information Assurance/Cyber Security regulations applicable to Marine Corps PKI Information Technology Systems to include Certificate Validation Infrastructure (CVI), Certificate Status Authority (CSA), Card Management System (CMS), Certificate Authorities (CAs), Registration Authority Workstations (RA workstations), Common Access Card Pin Reset Workstations (CPR-WS), and Certificate Validation Infrastructure Monitoring Tool (CVImon). The contractor shall provide support in the following areas:

The Contractor shall identify support personnel to serve as the PKI Cyber Security Compliance staff assigned under this subtask area.

a. Certification and Accreditation

The contractor shall ensure that all USMC PKI System Certification and Accreditation documentation is properly maintained to include:

- Register and maintain C&A activity concerning USMC PKI systems within the Marine Corps Certification and Accreditation and Support Tool (MCCAST)
- Coordinate annual re-certification and risk management assessments with 3.4 Plan, initiate, and monitor DIACAP/RMFDODIT MCCAST projects as required for new PKI system deployments.
- Coordinate the consolidation of required C&A documents within MCCAST with 3.2 and 3.4
- Create, maintain and update C&A Plan of Actions and Milestone (POA&M) documentation supporting continuous maintenance of ATOs

b. Security Configuration Compliance Management

The contractor shall ensure that all USMC PKI systems are properly configured in accordance with Security Technical Implementation Guides (STIG), Security Requirements Guides (SRG), and applicable vendor hardening guides. The contractor shall:

- Ensure no less than 20% of assets are evaluated monthly against DISA approved SCAP benchmarks applicable to each asset with 100% of all assets evaluated every six months and provide completed STIG checklist to Government leadership.
- Ensure that all assets are evaluated against the manual STIG checks applicable to each system every 12 months and provide completed STIG checklist to Government leadership.
- Direct resolution or document with a POA&M within 15 business days for Category I findings and 45 business days for Category II/III findings. Category I findings cannot be waived.
- Coordinate with EDM Global Policy Object managers, when required, in order to resolve deviations caused by GPOs
- Submit POA&Ms to the Information Assurance Manager (IAM) and/or Vulnerability Management Team (VMT) for Authorizing Official (AO) approval

c. Vulnerability Management

The contractor shall ensure that all USMC PKI systems are scanned for vulnerabilities in accordance with applicable operational orders and tasks as directed by USCYBERCOM, MARFORCYBER, local command authority, and as required by the MCCOG Information Assurance Manager.

- Ensure 100% compliance with the DoD Information Assurance Vulnerability Management system as directed by the Information Assurance Manager (IAM) and Vulnerability Management Team (VMT)
- IAVM findings must be resolved or documented with an IAVM POA&M submitted to the VMT within the proscribed reporting period

- Direct resolution or document non-IAVM findings with a POA&M within 15 business days for Category I findings and 45 business days for Category II/III findings. Category I findings cannot be waived.

d. Command Inspections

The Contractor shall provide support for the following periodic inspections: Computer Network Defense Service Provider (CNDSP) and Command Cyber Readiness Inspection (CCRI). The contractor shall:

- Support the Information Assurance Manager by providing PKI metrics for the CNDSP to include primary metrics and supporting documentation to metrics holders
- Support the Information Assurance Manager in the conduct of the CCRI ensuring PKI systems compliance with Vulnerability Scans, Security Technical Implementation Guides, Security Requirements Guides, and applicable vendor hardening guides
- Remediate PKI findings discovered by both the CNDSP and CCRI within proscribed limits set in accordance with post-inspection requirements

The Contractor shall update or develop and provide the following deliverables to support the Public Key Infrastructure Section. The documentation shall be developed using Government approved formats and with standard office automation software. The Contractor shall provide and use experienced technical writer support staff for required documentation with the assistance of the system Engineers and SMEs. Technical analyst support shall be provided and used for drafting and updating of all documentation. All installation and configuration documentation shall be managed under strict configuration controls. The Contractor shall establish and execute SOPs to ensure version control and adherence to sound configuration management practices for all documentation and solution artifacts.

- Instructions and Procedures for PKI Enterprise Solutions and systems to include:
 - Configuration Instructions
 - Installation Instructions
 - Maintenance Instructions
 - Transition Instructions
 - Release Instructions
 - Decommission/ Removal Instructions
 - End User Instructions
 - Engineering task, function, and process procedures
 - Standard Operating Procedures (SOPs)
- Design Documentation for PKI Enterprise Solutions and systems to include:
 - Detailed Technical Design
 - Detailed Configuration
 - Operating Guidelines
 - Implementation Guide
 - Diagrams and technical drawings (including logical, physical, wiring, data flow, and topological)
 - DIACAP documentation
 - Supporting attachments to enterprise design documents
 - Technical Requirements Documentation for PKI Services designs
- Supporting Documentation for PKI Enterprise Solutions and systems to include:
 - Plans of Action and Milestones (POA&Ms)
 - Test Plans
 - Certification and Accreditation (C&A) Documentation
 - Briefs and presentations
 - Engineering project management documentation
 - Written responses to Government tasks

- Completed Comment Resolution Matrixes (CRMs)
- Recommended policy documents supporting PKI enterprise designs and solutions
- Document templates
- Technical Training material and support documents
- Transition Plans
- Deployment Plans
- Documentation updates and rewrites
- Written assessments on requirements
- Configuration Management documents
- Lessons Learned Reports
- After-Action Reports
- Technology, practice, and product reviews and assessments
- Trip Reports
- Capacity and Availability Reports
- Participant notes and meeting minutes from all attendees shall be submitted to the Government within one business day after the activity for key meetings and all conferences
- Request for Modification (RFM) supporting documentation
- Request for Change (RFC) and incident tickets
- Release Plans and supporting documentation
- Implementation Plans
- Project and incident status reports
- Weekly status reports from each team member for all tasks and projects being worked
- Product Review & Evaluation Reports
- LRA Audit Reports
- USCYBERCOM/MARFORCYBER SIPR Reports
- Daily operations brief
- Additional supporting documents required from PKI Government Leaders

2.4.3 TASK 3 (OPTIONAL) - PROVIDE SURGE SUPPORT

On occasion the MCEN suffers periods of severe network incidents, outages, network attacks, natural disasters, and other operational shortcomings that require operations and disaster recovery actions beyond the capacity of normal staffing levels. The Contractor shall provide surge capability on short notice (within 14 calendar days of request) to provide additional support for Tasks 1 and 2 of this PWS. The Contractor shall provide support personnel that meet the minimum qualifications, as identified in the PWS, required for the task area/ subtask area that is being supported.

The Government may require the Contractor to distribute all or portions of the surge support among any of the above exercised task areas.

2.5 KEY PERSONNEL

2.5.1 The Contractor shall identify Key Personnel in accordance with the list below. Résumés for key personnel proposed for optional tasks shall be submitted for approval upon execution of that optional task.

2.5.2 The positions outlined below have been identified as key personnel positions and are subject to the substitution requirements as stipulated. The certification level held by the individual Contractors proposed to support task areas shall be clearly stated in the Key Personnel Qualification submissions and Staffing Matrix. Any personnel that are not certified at the time of award/appointment and throughout the duration of the Contract are considered unqualified.

The following table outlines Key Personnel requirements. The Key Personnel requirements are also stated in their corresponding task/subtask area:

Key Personnel (KP) – Qualification Table							
Billet Function	Task Area	Clearance	Preferred Tech Certification & Education	Minimum Tech Certification & Education	*Minimum Experience in Relevant Billet Function	8570 Requirements	**Estimated Percentage Augmentation Required
Program Manager	2.4.1	Top Secret	Professional level technical certification (e.g. CCNP or MCITP)	Bachelor's degree in a management related field Project Management Professional	10 Years General PM experience and demonstrated IT Related Project or Program Management	IASAE II	100%

Key Personnel (KP) – Qualification Table							
Billet Function	Task Area	Clearance	Preferred Tech Certification & Education	Minimum Tech Certification & Education	*Minimum Experience in Relevant Billet Function	8570 Requirements	**Estimated Percentage Augmentation Required
				(PMP) certification	Experience		
Network Operations Lead (KP)	2.4.2.4 2.4.2.5	Top Secret (SCI eligibility)		MCSE 2008 CISSP Axway Associates-level certification	10 years 7 years (PKI)	IAT 3	75%
Registration Authority	2.4.2.1	Secret	N/A	Technical Series Certification Security+ CE Key Recovery Registration Authority Certification CPR Reset ITILv3 Foundations	2 years	IAM 1	75%

Key Personnel shall provide support primarily for the task areas identified; however, Key Personnel may be required to support other MCCOG support tasks identified in this PWS as required by the Government.

2.5.3 The Contractor shall not substitute Key Personnel within the first one hundred and twenty (120) calendar days of the Contract performance period, unless such substitutions are necessitated by an individual's sudden illness, death, or termination of employment. In any of these events, the Contractor shall promptly notify the Contracting Officer (KO) in writing, and provide the information required as stated below. All proposed substitutions shall be submitted in writing to the KO. This written notification shall be submitted at least fifteen (15) calendar days, thirty calendar (30) days if a security clearance is to be obtained, in advance of the proposed substitutions to the KO. Any Key Personnel substitutions that are made within the first one hundred and twenty (120) calendar days of the Contract that do not fall under the exceptions listed may result in a negative past performance review.

2.5.4 All requests for substitutions must provide a detailed explanation of the circumstances necessitating the proposed substitutions; a complete résumé for the proposed substitute, and any other information requested by the COR. Key Personnel substitutions shall not be made without the KO

approval. All proposed substitutes shall have qualifications that are equal to or greater than the qualifications of the person being replaced. The KO shall evaluate such requests and promptly notify the Contractor of his/her recommendation. Should a replacement of key Personnel be required, the Contractor shall provide the Government with a copy of the replacement individual's résumé a minimum of 5 business days prior to making final selection of that individual. The Government shall have and will exercise its right to accept or reject the nominated individual.

2.5.5 In case of unsatisfactory Contractor performance, the Contractor shall take appropriate corrective action within ten (10) business days of formal notification to correct the problem as identified by the COR. In the event that the problem remains unresolved in excess of ten (10) business days, the Contracting Officer will recommend to the Contractor that appropriate action be taken; this may include employee removal from this Contract if warranted. The Program Manager shall ensure that all Government owned property and information are returned to the COR should a Contractor employee be removed.

2.6 SECURITY CONSIDERATIONS

2.6.1 Unless otherwise noted in the task area, all support staff providing services under this Contract shall possess at a minimum Secret level clearances. Unless stated otherwise, Interim Clearances are acceptable for normal processing of Clearance documentation for personnel with no current Clearance. Support staff must be able to maintain Clearance levels assigned to their tasks or the Contractor shall replace them with an individual that possesses the proper clearance.

The Contractor may be required, within short notice (14-30 days), to attain an upgraded clearance to support a changing security environment.

Before any subcontracting can take place, approval from the government representative is required.

The Contractor will utilize the Government Sensitive Compartmented Information Facility (SCIF) for all TS/SCI work as needed, see form DD-254 for specific locations authorized.

Security requirements are in accordance with the attached DD Form 254 and will be added as an attachment to the Contract upon award.

2.6.2 Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishing badges or other visible identification for meetings with Government personnel. Visible identification shall be worn at all times. In addition Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence.

2.6.3 The Contractor personnel will be required to access information systems such as the Navy Marine Corps Intranet (NMCI) or the MCEN and data accessed through portals via user accounts and Common Access Cards (CAC) that will be provided by the government. Contractor personnel must meet specific requirements IAW DoD 8570.1 Change, Information Assurance Workforce Improvement Program in order to be granted these privileges and maintain these credentials. Compliance with all USMC communications regulations IAW DoD 8570.1 Change, Information Assurance Workforce Improvement Program pertaining to network activities is mandatory. All Contractor personnel supporting this Contract shall be 8570 compliant. All key personnel and 65% of non-key personnel shall be 8570 compliant at the time of award. The remaining 35% of non-key

personnel shall have four (4) months from the date of Contract award to obtain required 8570 certifications. Once 100% 8570 compliance is reached, the Contractor shall maintain 100% 8570 compliance for the duration of the Contract. Any costs incurred by the Contractor to obtain and/ or maintain 8570 compliance shall be at no cost to the Government and is not billable to this Contract. Any new Contractor personnel shall be 8570 compliant at the start of their support on this Contract. Failure to comply with security requirements will result in revocation of access privileges and personnel removal from work under this Contract. If that is to occur, the Contractor shall provide an adequate replacement fully compliant with the requirements for the position.

2.6.4 Contractors with proper clearances shall be required to provide the following:

- JPAS visit request
- SF312 (Classified Information Nondisclosure Agreement)
- DD 2875 (System Authorization Access Request)

2.7 OTHER DIRECT COSTS (ODC) (TRAINING/ TRAVEL/ MATERIALS/ HOLA/ COLA)

Training and local and non-local/ long distance travel in support of Contract requirements within the continental United States (CONUS) and outside the continental United States (OCONUS) is authorized and may be required at the request of the Government. All non-local/ long distance travel, training, and material requests shall be submitted to the COR in writing prior to the Contractor incurring costs. COR approved ODCs to include non-local/ long distance travel, will be reimbursed at cost. Non-local/ long distance travel is defined within the Joint Travel Regulations. Any Government required travel incurred will be reimbursed at cost, in accordance with the Joint Travel Regulations. Prior to incurring cost for Government travel, estimate costs must be approved in writing by the COR. Training required to maintain the minimum technical certification and education requirements specified in this PWS is not an allowable ODC and will not be reimbursed by the Government.

2.8 GOVERNMENT-FURNISHED PROPERTY, FACILITIES, EQUIPMENT, INFORMATION (GFP, GFF, GFE, GFI).

2.8.1 Government furnished facilities or workspace will be provided at all required locations as a matter of routine. The Government shall provide, manage and hold custody of facilities, office furnishings, and equipment used by the Contractor in the performance of work under this Contract. The Government will provide the support staff with the workspaces, desks, telephones, ADP equipment, and software required to perform Contract tasks when and where necessary. The Contractor shall require all personnel to keep the spaces, furnishings and equipment provided for their use in a manner consistent with Marine Corps standards for fire prevention, health and safety; and takes proper care of all Government property in their possession.

2.8.2 The Marine Corps fully funds the subject effort; consequently, all reports, briefs, analyses, data and data products, models, tools, designs, training-related items, manuals, information, web-related and graphic works, software/script, and/or any other PWS-related items or materials, in whatever form, created, generated, produced, and/or delivered under the Contract (singularly or collectively referred to hereinafter as (Items)) and all associated intellectual property rights in or to the Items shall become the property of the Marine Corps and, therefore, the Marine Corps shall have the irrevocable, worldwide, royalty-free right to use, modify, reproduce, perform, display, release, or disclose such Items, in whole, or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so. This Contract shall include DFARS clause 252.227-7020. Therefore, any Items (including, but not

limited to Contractor and/or Third Party Proprietary data, information, software, and/or any other items or materials) that the Contractor intends to deliver to the Marine Corps with less than Unlimited Rights or do not meet the requirements of DFARS 252.227-7020 shall not be used for any work under this Contract \without the specific, written approval, by the Contracting Officer prior to start of any work. Releases and licenses, when required, shall be obtained and provided to the Contracting Officer.

2.8.3 The Marine Corps desires that all finished Items and end products created, generated, produced, and/or delivered under the Contract shall become the property of the Government, subject to Rights as expressed herein, and/or as modified in the Contract. This includes, but is not limited to, all items, data models, publications including, but not limited to, user's manuals and training materials, tools, reports, databases, presentation packages such as PowerPoint slides, computations with backup information, visual aids, meeting minutes and supporting documentation, instructions, and administrative tools, including but not limited to all hard copy and electronic versions, produced by the Contractor in the performance of the Contract. All materials, both hard copy and electronic, shall be maintained by the Contractor during the course of the Contract, and shall be turned over to the Contracting Officer at the conclusion of each program year, or more often upon request by the Contracting Officer.

2.8.4 The Contractor shall ensure that personnel accessing information systems have the proper and current IA certification to perform IA functions in accordance with DoD 8570, Information Assurance Workforce Improvement Program. All personnel performing tasks under this Contract shall be United States citizens. No foreign nationals shall be provided access to any Items any way associated with the effort under this Contract regardless of the security classification of such Items.

2.8.5 Upon completion or termination of this Contract, any Government furnished equipment, property, or Items provided to the Contractor shall be returned to the Government.

2.9 PERFORMANCE REQUIREMENTS SUMMARY (PRS).

The PRS is a listing of the tasks that will be monitored during the Contract term. The PRS Chart also lists examples of the types of documents that will be used during monitoring, as well as the standards of performance, the Acceptable Quality Level (AQL) of performance. All listings of required services or standards used in the PRS Chart are intended to be completely consistent with the terms and conditions of the PWS. This PRS also provides the minimum standard of acceptable performance as well as the minimum acceptable Quality level of this standard. Failure to meet the minimum AQL in any of the tasks listed will result in an assessment of unsuccessful performance for the task(s). Unsuccessful performance by the Contractor will result in a reduction in the monthly invoicing and payment amount to the Contractor. The reduction shall be taken from the CLIN of the respective task of which the Contractor is not meeting the standards. The amount reduced shall be calculated by multiplying the fixed price amount of the CLIN by the difference between the overall AQL for that task area and the overall assessed quality level for that task area.

2.10 Enterprise-wide Contractor Manpower Reporting Application (ECMRA).

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract **for MCCOG**, via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address <https://doncmra.nmci.navy.mil>.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at <https://doncmra.nmci.navy.mil>.

SECTION D

Packaging and Marking

There are no provisions in this section.

SECTION E

INSPECTION AND ACCEPTANCE

Pursuant to the inspection clause as provided in the master contract, all work described in the PWS to be delivered under this contract is subject to final inspection and acceptance by an authorized representative of the Government. The authorized representative of the Government is the Government's COR, who is responsible for inspection and acceptance of all services, materials, or supplies to be provided by the Contractor.

SECTION F

Deliveries or Performance

PERIOD OF PERFORMANCE

The period of performance shall be for a base period of six (6) months with one 6-month option period.

The option period may be exercised in accordance with FAR Clause 52.217-8 entitled "Option to Extend Services."

PLACE OF PERFORMANCE

See Attachment A.

REPORT(S)/DELIVERABLES AND DELIVERY SCHEDULE

The contractor shall submit all required report(s)/deliverables in accordance with the Performance Requirement Summary (PRS): All reports shall reference and cite the contract/order number.

SECTION G

Contract Administration Data

AUTHORITIES OF GOVERNMENT PERSONNEL

Notwithstanding the Contractor's responsibility for total management during the performance of this order, the administration of the order will require coordination between the Government and the Contractor. The following individuals will be the Government's points of contact during performance of the order.

Contracting Officer

Alexander Lyon
220 Lester Street
Quantico, VA 22134

Phone: (703) 432-7476

Email: alexander.lyon@usmc.mil

Contract Specialist

Natsaha Jones

2200 Lester Street

Quantico, VA 22134

Phone: (703) 432-7499

Email: natasha.jones@usmc.mil

Contracting Officer Representative

TBD

CONTRACTING OFFICER'S REPRESENTATIVE (COR) AUTHORITY

(a) Performance of work under this contract must be subject to the technical direction of the Contracting Officer's Representative identified above, or a representative designated in writing. The term "technical direction" includes, without limitation, direction to the contractor that directs or redirects the labor effort, shifts the work between work areas or locations, fills in details and otherwise serves to ensure that tasks outlined in the work statement are accomplished satisfactorily.

(b) Technical direction must be within the scope of the specification(s)/work statement.

The Contracting Officer's Representative does not have authority to issue technical direction that:

(1) Constitutes a change of assignment or additional work outside the specification(s)/statement of work;

(2) Constitutes a change as defined in the clause entitled "Changes";

(3) In any manner causes an increase or decrease in the contract price, or the time required for contract performance;

(4) Changes any of the terms, conditions, or specification(s)/work statement of the contract;

(5) Interferes with the contractor's right to perform under the terms and conditions of the contract; or

(6) Directs, supervises or otherwise controls the actions of the contractor's employees.

(c) Technical direction may be oral or in writing. The Contracting Officer's Representative shall confirm oral direction in writing within five work days, with a copy to the Contracting Officer.

(d) The contractor shall proceed promptly with performance resulting from the technical direction issued by the Contracting Officers, Representative. If, in the opinion of the contractor, any direction of the Contracting Officers, Representative, or his/her designee, falls within the limitations in (b), above, the contractor shall immediately notify the Contracting Officer no later than the beginning of

the next Government work day.

(e) Failure of the contractor and the Contracting Officer to agree that technical direction is within the scope of the contract shall be subject to the terms of the clause entitled "Disputes."

INVOICE SUBMISSION

The Contractor shall submit invoices once per month. A complete invoice with all required back-up documentation shall be sent electronically, via email, to Defense Finance and Accounting Service (DFAS) with a copy to:

1. Contract Specialist: natasha.jones@usmc.mil
2. Contracting Officer's Representative (COR): [TBD](#)
3. Financial Management Service (FMS): [TBD](#)

* No other non-invoice related documents (i.e. deliverables, reports, balance statements) shall be sent to the FMS mailboxes. Invoices Only.

The subject line of your email invoice submission shall contain the contract number, contract line item number, the order number, if applicable, and the number of invoices. The Contractor shall send one email per contract per month. The email may have multiple invoices for the contract. Invoices must be in the following formats: PDF, TIFF, or Word. No Excel formats will be accepted. The electronic file cannot contain multiple invoices; example, 10 invoices requires 10 separate files (PDF or TIFF or Word).

Invoices shall be submitted in accordance with the contract terms, i.e. payment schedule, progress payments, partial payments, deliverables, etc.

All calls concerning contract payment shall be directed to the COR.

In accordance with FAR 52.212-4, Contract Terms and Conditions-Commercial Items, a proper invoice must include the following items:

FAR 52.212-4(g) Invoice.

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include:

- (i) Name and address of the Contractor;
- (ii) Invoice date and number;
- (iii) Contract number, contract line item number and, if applicable, the order number;
- (iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
- (v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
- (vi) Terms of any discount for prompt payment offered;
- (vii) Name and address of official to whom payment is to be sent;
- (viii) Name, title, and phone number of person to notify in event of defective invoice; and
- (ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the

invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer, System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer, Other Than System for Award Management), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR Part 1315.

Additionally, the FMS requires the contractor to include its Dun & Bradstreet Number (DUNS) on each invoice.

In accordance with OMB Memorandum, M-11-32, Agencies shall make payments to small businesses as soon as practicable, with the goal of making payments within 15 days of receipt of a proper invoice. If a small business contractor is not paid within this (15 day) accelerated period, the contractor will not be given a late-payment interest penalty. Interest penalties, as prescribed by the Prompt Payment Act, remain unchanged by means of this memorandum. All small businesses shall label all invoices as "Small Business."

Additionally, in accordance with OMB Memorandum, M-12-16, all prime contractors are encouraged to disburse funds received from the Federal Government to their small business subcontractors in a prompt manner. To assist prime contractors in expediting contractor payments to small business subcontractors, Agencies shall, to the full extent permitted by law, temporarily establish an earlier, accelerated date for making agency payments to all prime contractors. Consistent with OMB Memorandum M-11-32 above, Agencies shall have a goal of paying all prime contractors within 15 days of receiving proper documentation. In an effort to support small business growth, drive economic activity and job creation, the Contractor is encouraged to accelerate payments to their small business subcontractors.

In accordance with the requirements of the Debt Collection Improvement Act of 1996, all payments under this order will be made by electronic funds transfer (EFT). The Contractor shall provide financial institution information to the Finance Office designated above in accordance with FAR 52.232-33 Payment by Electronic Funds Transfer - System for Award Management

SECTION H

Special Contract Requirements

CONTRACTOR PERFORMANCE EVALUATION(S)

During the life of this contract, Contractor performance will be evaluated on an interim and final basis pursuant to FAR Subpart 42.15. The Contractor Performance Assessment Reporting System (CPARS) will be utilized for these reviews. Information on CPARS can be located at <http://www.cpars.gov>.

7.2 SERVICE CONTRACT ACT WAGE DETERMINATIONS

All applicable labor categories must follow the Service Contract Act Wage Determinations. The Contractor is bound by the Wage Determination Number 2005-2103, Rev. 15, dated 12/22/2014, and all subsequent revisions made under this Wage Determination Number, issued by the U.S. Department of Labor, in accordance with the Service Contract Act of 1965, as amended (41 U.S.C. 351). The Contractor is put on notice that after performance begins, the Contractor is responsible for paying employees at least the applicable wage determination rate, if one exists, for the place of performance. The Department of Labor strictly enforces the Service Contract Act for all employees covered by the Act. The above referenced Wage Determination Number is for the Washington D.C. geographical area. If the place of performance is other than this geographical area; and therefore changes this Wage Determination Number the award will include the appropriate revised number, as necessary. Service Contract Act Wage Determinations can be found at <http://www.wdol.gov/>.

SECTION J

Attachments

- Attachment A: PKI Locations and Hours of Support
- Attachment B: PKI PRS and QASP
- Attachment C: Labor Hour Price Schedule
- Attachment D: DD254
- Attachment E: Wage Determination